AK

Notice of Allowability	**Application No.** 10/750,340	**Applicant(s)** AISSI ET AL.	
	Examiner Samson B. Lemma	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *amendment after non-final filed on 10/16/2007*.

2. ☒ The allowed claim(s) is/are *1-5,7-10,12-15,25-30 and 34-36*.

3. □ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) □ All b) □ Some* c) □ None of the:
   1. □ Certified copies of the priority documents have been received.
   2. □ Certified copies of the priority documents have been received in Application No. _____ .
   3. □ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. □ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. □ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) □ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
   1) □ hereto or 2) □ to Paper No./Mail Date _____.
   (b) □ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. □ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. □ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 10/16/2007
4. □ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. □ Notice of Informal Patent Application
6. □ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. □ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. □ Other _____.

DETAILED ACTION

1. This office action is in reply to an amendment filed on October 16, 2007. **Claims 6, 11, 16-24 and 31-33** are canceled. All independent claims namely **Claims 1, 8, 25 and 28 are amended**. New dependent claims 34-36 are added. Thus claims 1-5, 7-10, 12-15, 25-30 and 34-36 are pending / examined.

2. In the pervious office action **claims 25-33** were rejected under 35 U.S.C. 101 because the subject matter is directed to non-statutory subject matter, however Applicant's representative amended the specification on paragraph 0128 of the Published specification or the equivalent (page 35, lines 27-29) of the original specification and overcomes the rejections. Therefore the 35 U.S.C. 101 rejection set forth in the previous office action is withdrawn.

3. In the pervious office action, Examiner objected dependent claims **6-7 and 11-15** as being dependent upon a rejected base claim, and indicated that these dependent claims would be allowable if rewritten in independent form including all the limitations of the base claim and any intervening claims. Accordingly, Applicant's representative canceled some of the dependent claims and incorporated them in each independent claim.

Priority

4. This application does not claim priority. Therefore, the effective filling data for the subject matter defined in the pending claims of this application is **12/31/2003.**

Allowable Subject Matter

5. **Claims 1-5, 7-10, 12-15, 25-30 and 34-36 are allowed.**

6. The following is an examiner's statement of reasons for allowance:

Referring to the independent claims, the reference on the record, Trostle discloses a method comprising:

Performing an authentication *[Figure1 and figure 3]* **of a computing device** *[figure 1, ref. Num "100"/client]* **and equipment of an operator of services for the computing device** *[figure 1, ref. Num "102"/SERVER]* **for a session of communication between the computing device and the equipment,** *[figure 1, ref. "104", "106", "108" and "110" or see also figure 3]* **the performing comprising:**

- **Generating, in the computing device** [figure 1, ref. Num "100"/client], **a random number;** *[column 5, lines 34-35 and figure 1, ref. Num "104", see "c"] (On column 5, lines 34-35 and on figure 1, ref. Num "104", c the following has been disclosed. "Additionally, C/Client 100 generates random values for authenticators c and s.")*

- **Generating a one-time-pad key based on a hash operation of a value** *[Column 5, lines 31-33, "$DHKey_1$" or K which is the hash of encryption key k see column 4, lines 50-51]* **based on operation of a value selected from the group consisting of an identification of the computing device** *[$DHkey_1=Y_1^{x1}$ mod p, notice that x1 the private Diffie-Hellman values of the computer device or the client or K/one-time-pad key is the hash value of the secret password]* **an identification of the equipment** *[$DHkey_1=Y_1^{x1}$ mod p, notice that Y1 the public Diffie-Hellman values of the equipment/server]* **,stored in a protected storage within the computing device** *[See Table 2 and column 5, lines 1-2, "Both the client/computing device 100 and the server/Equipment102 store the current shared private key] (Furthermore see column 5, lines 20-35] and*

- **Encrypting the random number based on the one-time-pad key** *[See figure 1, ref. Num "104" and column 5, lines 42-44, "while y1 and s are encrypted with K and the hashed value of c is encrypted with $DHkey_1$"];*

- **Transmitting the encrypted random number to the equipment** *[See figure 1, ref. Num "104" and column 5, lines 35-38, "client/c/ computing device 100 sends the msg 104 to the Server 102/equipment];*

- **Receiving, from the equipment [Figure 1, ref. Num "102"], an encrypted value [column 5, lines 54-58] in response to the encrypted random number, wherein the encrypted value includes a challenge of a challenge-response** *(See on figure 1, ref. Num, "106" or see also on column 5, lines 54-58, msg 106 notice that [s, Y_2] is encrypted by $DHkey_1$ And THIS IS SEND FROM THE SERVER 102/EQIPMENT AND SEND TO THE CLIENT/COMPUTING DEVICE, INOTHER WORDS IT IS RECIVED FROM THE EQUIPMENT/SEVER 102);*

- **Verifying the encrypted value [Column 5, lines 60-65)** *(When C/client or computing device 100 receives message 106, C, it decrypts message 106 to obtain s and Y.sub.2. C 100 uses s in message 106 to authenticate S. Specifically, C 100 compares the value of s sent in message 104 with the value of s decrypted in message 106. If the two values are the same, C 100 knows that S 102 sent the message, since only C 100 and S 102 know K);*

- **Encrypting a response to the challenge of the challenge-response ; transmitting the response to the equipment** [See figure 1, ref. Num "108" and column 6, lines 17-19,see msg "108"]; **and receiving, from the equipment, an authentication verification** [figure 1, ref. Num "110", column 6, lines 23-35] .

Trostle does not explicitly disclose

Auditing the authentication, wherein auditing comprises:

Storing at least one attribute of the authentication into an audit log within a memory of the computing device;

Encrypting the audit log based on an encryption key that is generated and stored within the computing device;

Generating an integrity metric of the audit log; and

Generating a signature of the integrity metric with a signature key that is generated and stored within the computing device

However, **Ogg the new reference found**, generally discloses some of the following limitation

Auditing the authentication, wherein auditing comprises:

- **Storing at least one attribute of the authentication into an audit log within a memory of the computing device***[Column 11, lines 59-67 and column 12, lines 1-3];*

- **Encrypting the audit log based on an encryption key that is generated and stored within the computing device [column 12, lines 15-26**; column 18, lines 25-29 and column 20, lines 50-59]

- **Generating an integrity metric of the audit log** *[Column 43, lines 1-27; column 11, lines 59-67 and column 12, lines 1-3]*; and

- **Generating a signature of the integrity metric with a signature key that is generated and stored within the computing device** *[Column 43, lines 1-27; column 11, lines 59-67; column 12, lines 1-3]*

- However **the combination of Trostle and Ogg** does not explicitly disclose each and every functional limitation which was added to the respective independent claims together with the other limitation recited in the respective independent claims.

For this reason, independent claims **1, 8, 25 and 28**_are allowed.

7. The dependent **claims** which are dependent on the above **independent claims** being further limiting to the independent claims, definite and enabled by the specification are also allowed.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submission should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.(See PTO-Form 892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private

PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA
S.L.
12/17/2007

Gilberto B
GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100